International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)

ISSN: 2456-236X

Vol. **04** Issue **02** |2020

Security Based protocol for Protection of Patient Health Records on Cloud using Cipher Text Based Policy for Sign-Encryption and Decryption of Records through Email.

[1]*Mayank Shankar*

[1]*Jain University, Bangalore, 560069, India*

ABSTRACT

Cloud Data Storage plays an important role in managing and storing millions of data worldwide- From Business to Technology, Entertainment purposes, cloud Storage and many more services use cloud services to manage their data because it simplifies the way of storing and using the stored data. Whether it's an IaaS, PaaS or SaaS service all play vital roles in their respective areas. But the most important part is how secure are our private data on cloud. This paper focuses on security of Patients Health Record on the cloud. Now talking about Security of patients' health records it can be carved out from sources that it's is a patient centric model of data records of exchanging health information between the data sender's Ip address and the data receiver ip address using electronic means. [1]

Keyword: Cloud, Ip address, Cipher Text, Asymmetric Encryption, Public and Private Key

1. INTRODUCTION

Advanced technology has become the integral part of our life [2]. To satisfy the need of the society, almost in each work, we use the technology [3] [4]. In current era computer science is major subject [5]. It has many real life applications such as cloud computing [6], artificial intelligence [7], remote monitoring [8], Wireless sensor network [9, 10, 11], internet of things [12, 13, 14], Neural network [15, 16], FSPP [17, 18, 19], NSPP [20, 21, 22, 23, 24], TP [25, 26, 27], internet Security [28], uncertainty [29, 30, 31, 32, 33] and so on. Technology is the mode by which user can store, fetch, communicate and utilize the information [34]. So, all the organizations, industries and also every individual are using computer systems to preserve and share the information [35] . The internet security plays a major role in all computer related applications. The internet security appears in many real-life applications, e.g., home security, banking system, education sector, defense system, Railway, and so on. In this manuscript we discuss about the protection of authentication which is a part of internet security.

Health is the most valuable aspect of every human being residing all around the world. The most important point is we start to understand only if we feel that there's a threat losing it. Since the world has starting using electronically medical records, we see that Healthcare data records security has become one of the valuable aspects of Data Protection. Following the data from recent time's hackers' interest in electronically medical records has increased. This health care information is much more important than the credit card details or bank account passwords at the black market. Hackers or Fraudsters can gain access to the medical records that can contain the following crucial information of the patients: [3] [36]

1. Name of the patient
2. Date of Birth.
3. Mobile Number
4. Place of Work, Their job positions.
5. ID Card details, Medical and Health insurance/Social Insurance details.

This whole research paper will focus on security of Patients health records taking the following points into consideration:

1. How Security can be important for HealthCare data security.
2. Why it is important.
3. Role of Cipher text policy implemented into this paper
4. How Asymmetric Encryption is used to Encrypt and Decrypt the data using public and private key. [2] [37]

Role of fraudsters in using the stolen electronic medical data health records for personal or destructive needs.

1.1 Trying to receive medical health treatment using the personal expense of other patients.

Treatment in Hospitals has their own cost of treatment. Some are of low costs yet some are expensive. Physicians Take Important care of these services but in case fraudster gets the private data it can damage the patient's financial services and Personal insurance/social insurance.

1. 2 Scheming plot with medicines:

Fraudsters that don't need any medical treatment and are completely fit can receive a good amount of money byordering Expensive drugs on behalf of medical cardholders aiming to retrieve those and then resale them gaining theirownprofit Maximization.

1.3 Plotting a conspiracy with employees of clinic or hospitals

If the Criminals manage to get into touch with amoral clinic employees, the insurance company can be billed for the services that they have never come across or never used and the cash will be divided among the reprobated clinical employees and the Fraudsters.

2. MEDICAL HEALTH DATA BREACHESBRIEFING AND INSIGHT

2.1 Data Breach Brief:

Health Data Breaches continue to effect healthcare industry till 2018 with around 488 incidents which affected almost 14.78million patient records. The total number of affected records from 2017 which recorded457data breaches affecting 5.49 million records. Insiders belonging to HealthCare industry were responsible for around 144 breaches in 2016, which slightly. Reduced down from183 in 2017. Out of those 92 cases involved cases from an inside error and 47 were involved in insider Misconduct. [4] [38]

2.2 Data Breach Insight:

Data breaches cost healthcare organizations a loss of more than the total loss arising from various service interruptions and potential HIPPA (Health Insurance Portability and Accountability Act) fines, which can be somewhat sturdy causing harm towards the brand of the image and affecting and forcing customers to take their business and medical care somewhere else. Yet there are various security vulnerabilities of EHR (Electronic Health Records) and insufficient funds for cyber security purposes continuing to put many health organizations and other systems at risk, often originating from inside employees PROTENUS [39] a popular health care compliance analytics platform records a case in 2018 where a medical assistant printed the details of patients and gave information to people who used them to commit crimes. Medical assistants allegedly racked more than $35,000 in unemployment benefit before getting into the hands of law.2/3 of Inside Data Breaches(69.45%) involved snooping onto a family member and around 52% where offenders repeated.[4][38]

3. PRIVACY, CONFIDENTIALITY AND SECURITYOF HEALTHCARE INDUSTRY

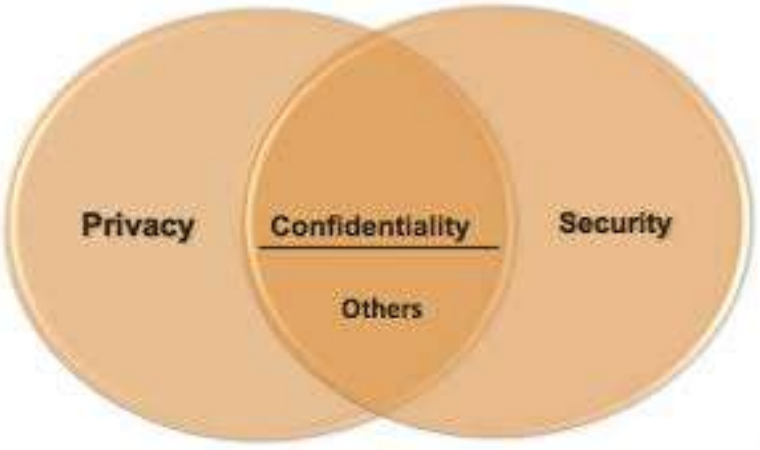

Fig.1 GOAL: Patient confidentiality, privacy, security [40]

3.1 Confidentiality

People responsible for patient confidentiality

- Brand Members
- Executive Leadership
- Clinical Staff
- Physicians and Nurses
- Administrative and Clerical Staff
- Students / Interns
- Volunteers

List of patient's information kept confidential

- Identity(Name, Address, Social, Insurance)
- Physical condition
- Emotional condition
- Financial Information

Confidentiality Principles

- Don't leave any patient records or files unattended
- Accessing patient's information only when required and not for self-purposes.
- Discarding confidential information upon use.
- Reporting Suspicious Activities to Privacy Officer

3.2 Privacy

Purpose of HIPPA (Health Insurance Portability and Accountability Act)

- Improving efficient and effectiveness of health care system
- Encouraging development of EHR.
- Establishing National Standards for electronically generated transmission of health information and protecting them
- Ensuring the confidentiality of patient
- Protecting the privacy of patients.
- Building the loyalty and trust with Health Workers
- Providing required Health Related Customer Service on cloud.

3.3 SECURITY

- Protecting Patients Data helping in building trust between patients and Electronic Health Information Administrator.
- PHI (PROTECTED HEALTH INFORMTION) should act be disclosed to unauthorized persons.
- Avoiding sending emails containing PHI if it is not encrypted.
- If suspecting some strange acts of fraud immediately contact the official help desk
- Build Strong Passwords using all Characters. Numbers and symbol.[6][41]

4. IMPLEMENTATION DESIGN OF THE PROJECTWORK DONE

4.1. Data Flow Diagram:

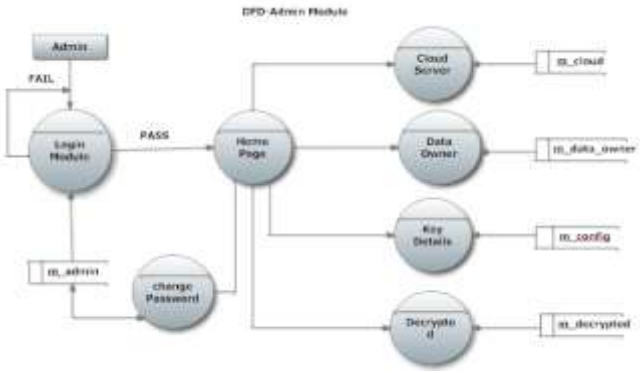

Fig. 2 Admin Session

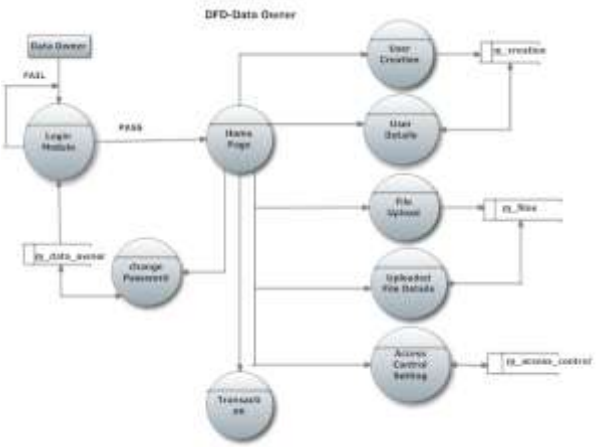

Fig. 3 Data Owner

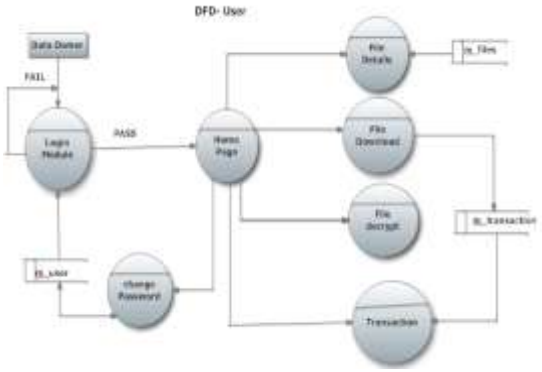

Fig. 4 User account control

4.2 Use Case Diagram

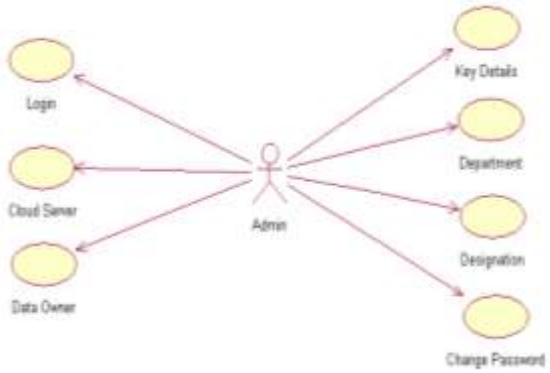

Fig. 5 Admin Module Details

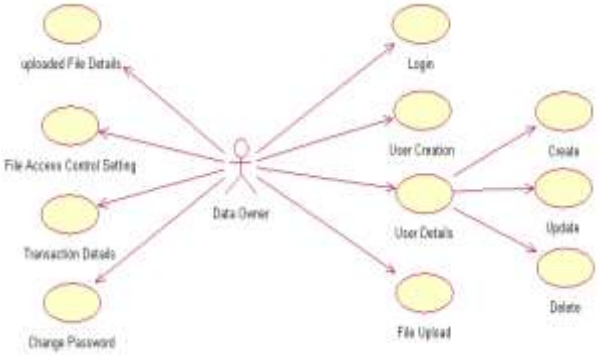

Fig. 6: Data Owner Account Modules

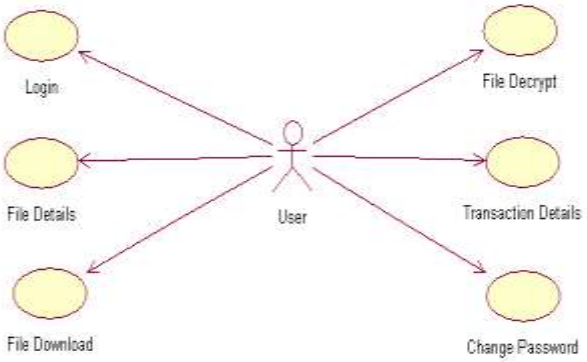

Fig. 7: User Account Details

4.3 Sequence Diagram: To Download the File

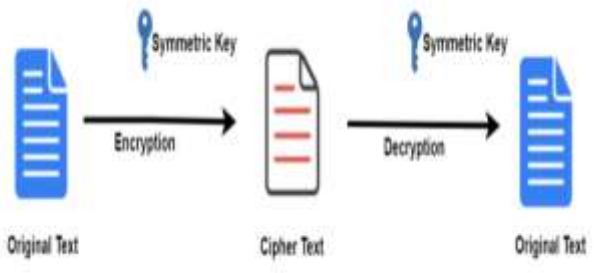

Fig. 8. Key Encryption and Decryption

Both data sender and the data recipient must remember their secret key which is required to encrypt or decrypt all the
Messages. The Following Symmetric encryption can be used:

- Blowfish
- Rivets Cipher (RC4)
- Advanced Encryption Standard - AES 128, AES 192, AES 256
- Data Encryption Standard (DES)
- Rivets Cipher 5 (RC5)
- Rivets Cipher 6 (RC6) [7][42]

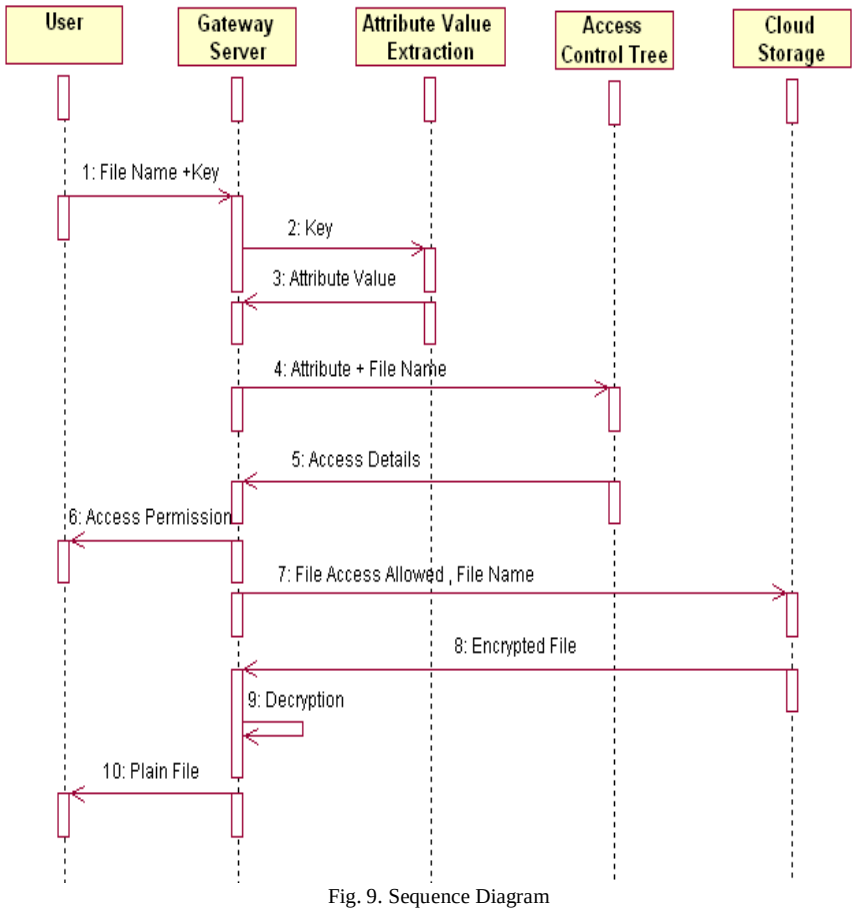

Fig. 9. Sequence Diagram

5. KNOWLEDGE IMPLEMENTED IN THE PAPER

5.1 Symmetric Encryption

The simplest encryption method where same key is required to encrypt message into cipher text and then decrypt the ciphertext to original message.

ISSN: 2456-236X

Vol. **04** Issue **02** |2020

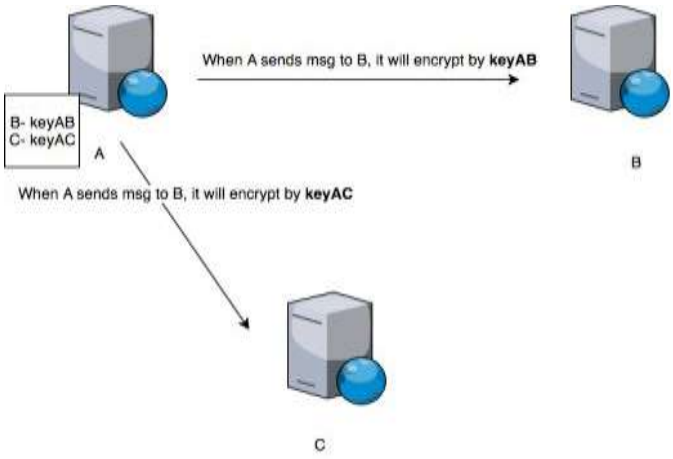

Fig. 10 Encryption Process

5.1.1 Process Involved In Encryption

Let us assume person A as Mayank and Person B as Dolly.

Mayank sends the decrypted message to Dolly, now Mayank will encrypt this message with his key AB and resends the key with a message to Dolly. So Dolly can now be able to decrypt this message using her key. Similarly when Mayank sends the same message to Ash, then Mayank will need to encrypt the message with key (AC) and then finally send the Cipher Text and the key. Then C decrypts the Cipher Text by using the key sent by Mayank.

5.2 Asymmetric Encryption

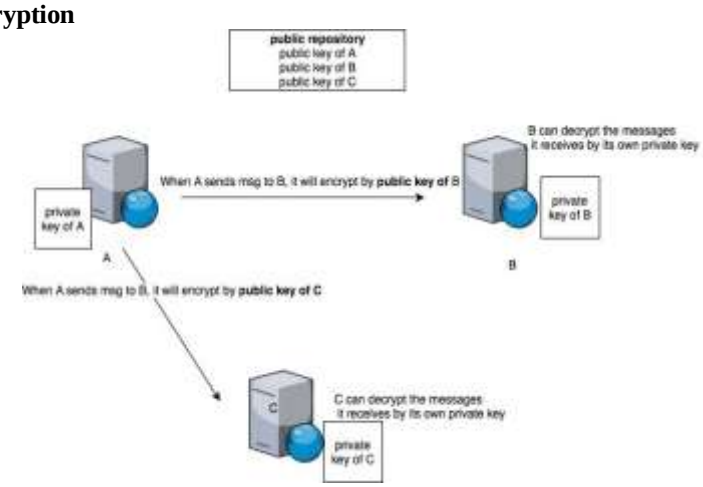

Fig. 11 Asymmetric Encryption

The Public Repositories present in the Encryption and Decryption process are:

- ✓ Public Key of A (Mayank)
- ✓ Public Key of B (Dolly)
- ✓ Public Key of C (Yash)

Mayank sends encrypted message to Dolly, this message gets encrypted by public key Dolly has with her. Now Dolly will decrypt the message received by her owned private Key. Similarly when Mayank sends Message to Dolly, it will get encrypted by public key owned by Yash. Finally Yash decrypts the message he receives by his own private key

6. CONCEPT IMPLEMENTED IN THIS PAPER

Since asymmetric encryption is more secured than symmetric encryption since it has different keys for both encryption and decryption this paper is completely based on asymmetric encryption. The complete process is explained by the below diagram.

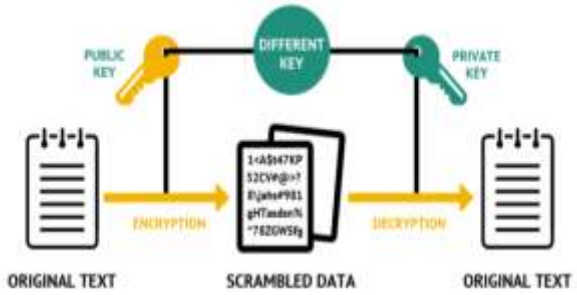

Fig. 12Data Exchange Using Cipher Text

Asymmetric Encryption uses different encrypted keys for both Encryption and Decryption process of files. This is also known to the world as Public Key Cryptography.

The Secret key involved in Encryption and Decryption are exchanged over the internet or a very large network. Asymmetric encryption always ensures that unwanted person cannot misuse the key. It involves two keys. [8] [43]

- Private Key
- Public Key


Fig. 13Private and public keys

Private Key is owned only by it's the person who has the hashed key. This key is always kept confidential to him. Let us assume that Dolly has her private key, Cipher Text algorithm says that for every private key there's a public key. A person can gain access to everyone's public key. So Dolly can send her public key to Mayank. This public key is publically accessible to everyone. A message encrypted using public key can be decrypted only using its private key. Public key does not need to be secured since it is available to the public. So it can be shared over the internet

7. SIGNING AND VERIFICATION PROCESS

7.1 **Why Include Signatures:**

Signature is used for authentication of files and documents. By using signatures Dolly makes sure that the required documents are sent by Mayank and each and every information which is shared are finally approved and verified by Dolly. As in asymmetric encryption here also two key pairs are available, a public key and private key. Since the private key is owned by the person who has the hashed key, we can use it for signing. When Dolly wants to share information or a message to Mayank, Dolly will encrypt the message using her private key. Now Dolly sends message tomahawk over the network. Mayank already has Dolly's public key. So he can decrypt the message using Dolly's public key and a validation message is sent to Dolly since private key of Dolly is unique to herself and no other person can own that key.

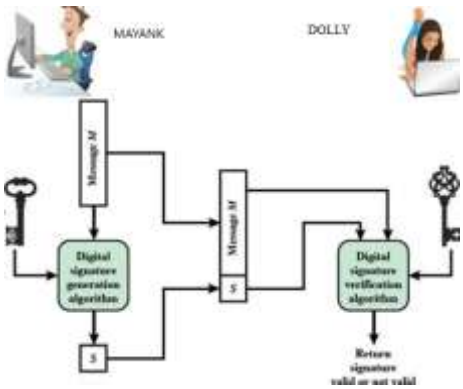

Fig. 14Message Sending Between A and B

7.2 How Signatures ARR Processed

- When Dolly wants to send message to Mayank, He takes the message and hashes the message.
- Dolly will encrypt the message using his private key.
- Dolly will now combine her original message and the hashed message together and then encrypt it using public key of Mayank.
- Now Dolly sends the message to Mayank.

7.3 How Signed Document Verification Is Done

- Mayank receives the message. He will decrypt the complete message using his own private key.
- Inside the message two components reside: original message and the hashed message which is encrypted by Dolly's Private Key.
- Then Mayank hashes the original message using hash algorithm used by Dolly. Now Mayank has the hashed text of the original message.
- Finally Mayank decrypts the hashed text that was previously sent by Dolly using her public key and then compares it with official message hashed by Mayank. Now Mayank can verify the message sent by Dolly

8. CONCLUSION

We come to the final conclusion that how important patient's health data records are when it is operated electronically. Every time the main highlighted point is its security. Cipher Text follows transforming encrypted text from plain text using and encryption algorithm as discussed before. Public key and private key have been used to encrypt the data from its hashed form to the original message. When the Administrator wants to send the patient health records to the patients he sends a decrypts the message and then send to the email id of the message. Both the patient and the administrator have their own private key. The patients receive the decrypted key and then copies and paste the key on the document access page that requires the key. After inserting the decrypted key the patient can view his health condition and other required information. Sending the decrypted key to the email of the person is important because each and every person has their private access and no one else can use it not even the administrator. So it ensures better security for managing health records by clinics and Hospitals.

9. REFERENCES

[1] D. Rani and R. K. Ranjan, "A Comparative study of SaaS, PaaS and IaaS in cloud Computing," ijarcsse, vol. 4, no. 6, p. 4, June 2014.
[2] M. BM and H. Mohapatra, "Human centric software engineering," International Journal of Innovations & Advancement in Computer Science (IJIACS), vol. 4, no. 7, pp. 86-95, 2015.
[3] H. Mohapatra, C Programming: Practice, Vols. ISBN: 1726820874, 9781726820875, Kindle, 2018.
[4] H. Mohapatra and A. Rath, Advancing generation Z employability through new forms of learning: quality assurance and recognition of alternative credentials, ResearchGate, 2020.
[5] H. Mohapatra and A. Rath, Fundamentals of software engineering: Designed to provide an insight into the software engineering concepts, BPB, 2020.
[6] V. Ande and H. Mohapatra, "SSO mechanism in distributed environment," International Journal of Innovations & Advancement in Computer Science, vol. 4, no. 6, pp. 133-136, 2015.
[7] H. Mohapatra, "Ground level survey on sambalpur in the perspective of smart water," EasyChair, vol. 1918, p. 6, 2019.
[8] H. Mohapatra, S. Panda, A. Rath, S. Edalatpanah and R. Kumar, "A tutorial on powershell pipeline and its loopholes," International Journal of Emerging Trends in Engineering Research, vol. 8, no. 4, 2020.
[9] H. Mohapatra and A. Rath, "Fault tolerance in WSN through PE-LEACH protocol," IET Wireless Sensor Systems, vol. 9, no. 6, pp. 358-365, 2019.
[10] H. Mohapatra, S. Debnath and A. Rath, "Energy management in wireless sensor network through EB-LEACH," International Journal of Research and Analytical Reviews (IJRAR), pp. 56-61, 2019.
[11] H. Mohapatra and A. Rath, "Fault-tolerant mechanism for wireless sensor network," IET Wireless Sensor Systems, vol. 10, no. 1, pp. 23-30, 2020.

[12] H. Mohapatra and A. Rath, "Detection and avoidance of water loss through municipality taps in india by using smart tap and ict," IET Wireless Sensor Systems, vol. 9, no. 6, pp. 447-457, 2019.
[13] M. Panda, P. Pradhan, H. Mohapatra and N. Barpanda, "Fault tolerant routing in heterogeneous environment," International Journal of Scientific & Technology Research, vol. 8, pp. 1009-1013, 2019.
[14] D. Swain, G. Ramkrishna, H. Mahapatra, P. Patra and P. Dhandrao, "A novel sorting technique to sort elements in ascending order," International Journal of Engineering and Advanced Technology, vol. 3, pp. 212-126, 2013.
[15] H. Mohapatra, "HCR using neural network," 2009.
[16] V. Nirgude, H. Mahapatra and S. Shivarkar, "Face recognition system using principal component analysis & linear discriminant analysis method simultaneously with 3d morphable model and neural network BPNN method," Global Journal of Advanced Engineering Technologies and Sciences, vol. 4, p. 1, 2017.
[17] R. Kumar, S. Edalatpanah, S. Jha, S. Gayen and R. Singh, "Shortest path problems using fuzzy weighted arc length," International Journal of Innovative Technology and Exploring Engineering, vol. 8, pp. 724-731, 2019.
[18] R. Kumar, S. Jha and R. Singh, "A different approach for solving the shortest path problem under mixed fuzzy environment," International Journal of fuzzy system Applications, vol. 9, no. 2, pp. 132-161, 2020.
[19] R. Kumar, S. Jha and R. Singh, "Shortest path problem in network with type-2 triangular fuzzy arc length," Journal of Applied Research on Industrial Engineering, vol. 4, pp. 1-7, 2017.
[20] S. Broumi, A. Dey, M. Talea, A. Bakali, F. Smarandache, D. Nagarajan, M. Lathamaheswari and R. Kumar, "Shortest path problem using Bellman algorithm under neutrosophic environment," Complex & Intelligent Systems, vol. 5, pp. 409--416, 2019.
[21] R. Kumar, S. Edalatpanah, S. Jha, S. Broumi, R. Singh and A. Dey, "A multi objective programming approach to solve integer valued neutrosophic shortest path problems," Neutrosophic Sets and Systems, vol. 24, pp. 134-149, 2019.
[22] R. Kumar, A. Dey, F. Smarandache and S. Broumi, "A study of neutrosophic shortest path problem," in Neutrosophic Graph Theory and Algorithms, F. Smarandache and S. Broumi, Eds., IGI-Global, 2019, pp. 144-175.
[23] R. Kumar, S. Edalatpanah, S. Jha and R. Singh, "A novel approach to solve gaussian valued neutrosophic shortest path problems," International Journal of Engineering and Advanced Technology, vol. 8, pp. 347-353, 2019.
[24] R. Kumar, S. Edaltpanah, S. Jha, S. Broumi and A. Dey, "Neutrosophic shortest path problem," Neutrosophic Sets and Systems, vol. 23, pp. 5-15, 2018.
[25] R. Kumar, S. Edalatpanah, S. Jha and R. Singh, "A Pythagorean fuzzy approach to the transportation problem," Complex and Intelligent System, vol. 5, pp. 255-263, 2019.
[26] J. Pratihar, R. Kumar, A. Dey and S. Broumi, "Transportation problem in neutrosophic environment," in Neutrosophic Graph Theory and Algorithms, F. Smarandache and S. Broumi, Eds., IGI-Global, 2019, pp. 176-208.
[27] J. Pratihar, S. E. R. Kumar and A. Dey, "Modified Vogel's Approximation Method algorithm for transportation problem under uncertain environment," Complex & Intelligent Systems (Communicated).
[28] J. Sakhnini, H. Karimipour, A. Dehghantanha, R. Parizi and G. Srivastava, "Security aspects of Internet of Things aided smart grids: A bibliometric survey," Internet of Things, pp. 100-111, 2019.
[29] S. Gayen, F. Smarandache, S. Jha and R. Kumar, "Interval-valued neutrosophic subgroup based on interval-valued triple t-norm," in Neutrosophic Sets in Decision Analysis and Operations Research, M. Abdel-Basset and F. Smarandache, Eds., IGI-Global, 2019, p. 300.
[30] S. Gayen, F. Smarandache, S. Jha, M. Singh, S. Broumi and R. Kumar, "Introduction to plithogenic subgroup," in Neutrosophic Graph Theory and Algoritm, F. Smarandache and S. Broumi, Eds., IGI-Global, 2020, pp. 209-233.

[31] S. Gayen, S. Jha, M. Singh and R. Kumar, "On a generalized notion of anti-fuzzy subgroup and some characterizations," International Journal of Engineering and Advanced Technology, vol. 8, pp. 385-390, 2019.
[32] S. Gayen, F. Smarandache, S. Jha, M. K. Singh, S. Broumi and R. Kumar, "Introduction to plithogenic hypersoft subgroup," Neutrosophic Sets and Systems, vol. 33, p. Accepted, 2020.
[33] S. Gayen, S. Jha and M. Singh, "On direct product of a fuzzy subgroup with an anti-fuzzy subgroup," International Journal of Recent Technology and Engineering, vol. 8, pp. 1105-1111, 2019.
[34] Behura and H. Mohapatra, "IoT Based Smart City with Vehicular Safety Monitoring," EasyChair, vol. 1535, 2019.
[35] H. Panda, H. Mohapatra and A. Rath, "WSN-Based Water Channelization: An Approach of Smart Water," Smart Cities—Opportunities and Challenges. Lecture Notes in Civil Engineering, vol. 58, pp. 157-166, 2020.
[36] M. Oliynyk, "Why is healthcare data security so imporatant.," 2 March 2016. [Online]. Available: www.protectimus.com.
[37] L. Mohan, R. Pandey, S. Bisht and J. Pant, "A Comparative Study on SaaS, Paas and Iaas Cloud Delivery Models in Cloud Computing," NCETST, no. Special Issue, p. 3, 2017.
[38] M. Bryant, "Data Breaches Compromised," 13 February 2019. [Online]. Available: healthcaredive.com.
[39] H. Mohapatra, "APPROACHES AND CHALLENGES OF SMART CITIES OF INDIA," 2019.
[40] M. Kumar and S. Wambgu, "A primer on the privacy,security and confidentiality of electronic health records," February 2016. [Online]. Available: https://www.measureevaluation.org/resources/publications/sr-15-128-en.
[41] "Patient Confidentiality, Privacy and Security Awareness," privacyofficer@bmc.org, Boston.
[42] G. J. Simmons, "Symmetric and Assymetric Encryption," vol. 11, p. 26, December 1979.
[43] P. Paralogarajah, "Understanding Encryption, Signing and Verification," 22 February 2019. [Online]. Available: www.medium.com.